Computer virus - 007

संगणक विषाणू नियंत्रणाबाबत सूचना

महाराष्ट्र शासन,
सामान्य प्रशासन विभाग,
माहिती तंत्रज्ञान संचालनालय,
परिपत्रक क्रमांक : सीओएम-२००१/प्र.क्र.१५२/३९,
मंत्रालय, मुंबई. ४०० ०३२.
दिनांक : ०५ मार्च , २००२.

परिपत्रक :

प्रस्तावना :

मंत्रालय व परिसरातील कार्यालयांमध्ये साधारणपणे ३००० संगणक आणि राज्यात इतर शासकीय कार्यालयांमध्ये साधारणपणे ५००० संगणक कार्यान्वित करण्यात आलेले आहेत. असे निदर्शनास आले आहे की संगणकांवर विषाणूंचा (Virus) प्रादुर्भाव मोठया प्रमाणावर झाला असून त्यामुळे त्याचा संगणकांच्या कार्यक्षमतेवर परिणाम झालेला आहे. संगणक विषाणूंबाबत सर्वसाधारण माहिती, त्याचा प्रादुर्भाव झाल्याची सर्वसाधारण लक्षणे, विभागांनी त्याबाबत घ्यावयाची दक्षता, विषाणूंचे निर्मूलन इ. विषयी सविस्तर माहिती/मार्गदर्शक सूचना पुढे देण्यात आल्या आहेत.

१.१ संगणक विषाणू या विशिष्ट प्रकारच्या आज्ञावल्या संगणकाच्या सामान्य कार्यात दोष उत्पन्न करण्याच्या दृष्टीने लिहिलेल्या असतात. संगणकात विषाणूंचा प्रवेश संगणक संत्रणा व संगणक वापरणा-या व्यक्तिंच्या नकळतच होत असतो. विषाणूंचा प्रवेश मुख्यत्वे बाहेरील चुंबकीय तबकडी वापरल्याने , संगणकावर नकली सॉफ्टवेअर लोड केल्याने / वापरल्याने , पायरेटेड गेम्स लोड केल्याने अथवा फ्लॉपीद्वारे संगणकावर खेळल्याने इत्यादी कारणांमुळे होत असतो. बहुतेक सर्व संगणक विषाणूंमध्ये स्वत:च्या अनेक प्रतिकृती निर्माण करण्याची क्षमता असल्याने संगणकात एकदा विषाणूंचा प्रवेश झाल्यास विषाणू संगणकावर पसरत जातो व त्यामुळे संगणकाच्या सामान्य कार्यात विचित्रपणा उद्भवू शकतो. विषाणूंमुळे संगणकातील बूट रेकॉर्ड, अज्ञावल्या , डेटा फाईल्स व संगणकाच्या तांत्रिक भागात दोष उत्पन्न होऊ शकतात.

१.२ संगणक विषाणूची संख्या जवळपास ५८ हजाराच्या दरम्यान असून विषाणूंची कार्य शैली (Behaviour), संगणकात त्यांचे वास्तव्याचे ठिकाण (Location) व विषाणूंच्या प्रवेशाने संगणकाच्या सामान्य कार्यातील कार्यक्षमतेत होणा-या परिणामांनुसार विषाणूंची विभागणी मुख्यत्वे अ) प्रोग्रॉम/ फाईल्स विषाणू व ब) बूट सेक्टर विषाणू या दोन प्रकारात करण्यात आलेली आहे. फाईल्स विषाणू . EXE, .COM, Work file इ. फाईल्समध्ये असतात. काही विशिष्ट प्रकारच्या फाईल विषाणूंमध्ये डेटा फाईल्सनष्ट करण्याची क्षमता असते. जे विषाणू . EXE व .COM फाईल्समध्ये असतात त्यांचा मुख्य उद्देश स्वत:च्या अनेक प्रतिकृती निर्माण करणे हा असतो. बूट सेक्टर विषाणू बूट सेक्टरमध्ये असतात व ते संगणक बूट करतांना प्रत्येकवेळी कार्यान्वीत होत असतांना बूट सेक्टर व्हायरस असलेल्या संगणकावर चुंबकीय तबकडी (Floppy) वापरल्यास ती लगेचच दुषीत होण्याची शक्यता असते.

रेटा/एच-1080(1500-3-02)1

GR - 200204121555139000-010A

१.३ GUI टेक्नॉलॉजी, नकली (Pirated)पॅकेजेस, ई-मेल, इंटरनेट महाजाल, कॉम्प्युटर गेम्स इत्यादींमुळे व वाढत्या नकली सॉफ्टवेअर (Piracy) वापरामुळे दिवसेंदिवस नवीन विषाणू मोठया प्रमाणात पसरत आहेत. त्यात सूक्ष्म (Micro) व कृमी (Worm) विषाणूंचाही समावेश आहे. वर दिलेल्या विषाणूंच्या प्रकाराची नव्याने विभागणी प्रोग्राम विषाणू, बूट सेक्टर विषाणू, मल्टी पायरेटेड विषाणू, स्टिल्थ विषाणू व पॉलिमॉरफिक विषाणू अशा पाच प्रकारात करण्यात आली आहे. अशा नवीन विषाणूंचे निर्मूलन करणे अवघड असते व नवीन विषाणू निर्मूलनासाठी नवीन महागडे विषाणू निर्मूलन सॉफ्टवेअर विकत घ्यावे लागते. हे सर्व टाळण्यासाठी संगणकात व त्यावर वापरात येणाऱ्या चुंबकीय तबकडया व इतर मिडियांवर विषाणूंचा प्रवेश न होण्याबाबत सदैव जागृत राहून सातत्याने व कसोशिने प्रयत्न करणे आवश्यक आहे.

२. संगणकात विषाणूंचा प्रादुर्भाव झाल्यास खाली दिलेली लक्षणे निदर्शनास येऊ शकतात.

२.१ संगणकावर काम करत असताना संगणक बरेचवेळा मध्येच थांबतो (Hang) व की बोर्ड व माऊसला प्रत्युत्तर (Response) देत नाही.

२.२ संगणकाच्या मेन मेमरीमध्ये काम करण्याची जागा कमी होते. परिणामी मोठया फाईल्स उघडतांना अडचणी उद्‌भवतात. संगणकावर डॉस ऑपरेटींग सिस्टिम ६४० केबी एव्हढी मेमरी व्याप्त करते. ही व्याप्त केलेली बाईटस्‌ची संख्या विषाणूंमुळे कमी होऊ शकते.

२.३ Command.com ही डॉसची अत्यावश्यक फाईल असल्यामुळे या फाईलचा आकार(व्याप्ती) प्रमाणित केलेला असतो. आपल्या कार्यालयास पुरविण्यात आलेल्या संगणकावरील Command. com फाईलची व्याप्ती (आकार/Size) डॉसच्या ६.० व्हर्जनच्या आतील व्हर्जनसाठी ५४६४५ बाईट्स आणि ६.० ते ६.२२ च्या मधील व्हर्जनसाठी ९३८८० बाईट्स सदैव असावयास हवी. या फाईलचा आकार (व्याप्ती) कमी झाल्यास विषाणूंचा शिरकाव झाला असल्याची दाट शक्यता असते.

२.४ चुंबकीय तबकडीची(Floppy) क्षमता १.४४ एम.बी. (३.५") आणि १.२ एम.बी. (५.२५") एव्हढी निश्चित्त ठरलेली असते. काही संगणक विषाणू चुंबकीय तबकडीत असताना Dir कमांडने चुंबकीय तबकडीची क्षमता कमी वा अधिक झालेली आढळून येते.

२.५ विषाणूंमुळे ' फाईल ॲलोकेशन ' टेबल बरेचवेळा पुन्हा लिहिला जातो. त्यामुळे काही फाईल्स संपूर्णपणे अथवा अर्धवट नष्ट झालेल्या आढळू शकतात. विषाणूंनी प्रवेश केलेल्या फाईल्समध्ये विचित्र प्रकारची असंबध्द अशी चित्रेही आढळू येते.

२.६ संगणकाच्या कार्यक्षमतेत (मुख्यत्वे गतीत) एकदम बदल झालेला आढळतो. विषाणूंच्या प्रादुर्भावामुळे काही संगणित्रांकडून अतिशय हळू प्रतिसाद मिळतो.

२.७ संगणकावर सर्वसाधारणपणे आढळणाऱ्या संदेशा व्यतिरिक्त विचित्र संदेश (Strange Messages) अथवा विचित्र प्रकारच्या आकृत्या संगणकाच्या मॉनीटरवर आढळतात

वर नमूद केलेल्या बाबी संगणकावर काम करत असताना दिसून आल्यास संगणकावर विषाणूंचा प्रवेश झाला असल्याची दाट शक्यता असते. संगणकातील काही तांत्रिक भागात बिघाड झाल्यास सुध्दा वरील लक्षणे आढळून येऊ शकतात. तांत्रिक बाबी तज्ञांकडून तपासण्या अगोदर विषाणूंबाबत तपासणी तात्काळ करणे आवश्यक आहे व सदर तपासणी व विषाणूंचे निर्मूलन करण्याच्या दृष्टीने नॉर्टन (Norton) नावाचे विषाणू निर्मूलन सॉफ्टवेअर उपलब्ध करण्यात आलेले आहे. या सॉफ्टवेअर वापरासंबंधी सविस्तर सूचना पुढील काही परिच्छेदात देण्यात आल्या आहेत.

३. संगणकाचे विषाणूंपासून रक्षण करण्यासाठी पुढील कार्यवाही करणे आवश्यक आहे.

३.१ संगणक चुंबकीय तबकडीद्वारे (Floppy) शक्यतो बूट करू नये व तशीच गरज भासल्यास प्रथम बूटेबल चुंबकीय तबकडी (Floppy) शुद्ध अशी विषाणू विरहीत असल्याबाबत खात्री करून घेण्यात यावी.

३.२ आपल्या कार्यालयास उपलब्ध करण्यात आलेल्या चुंबकीय तबकडया (Floppy) व्यतिरिक्त इतर कुठल्याही कार्यालयातील चुंबकीय तबकडी वापरू नये. बाहेरील कार्यालयातील चुंबकीय तबकडी (Floppy) वापरावयाची गरज पडल्यास प्रथमत: ही चुंबकीय तबकडी (Floppy) विषाणू विरहित असल्याबाबत खात्री करून घेण्यात यावी.

३.३ आपल्या कार्यालयातील चुंबकीय तबकडी (Floppy) इतर कार्यालयास तात्पुरती देण्याची आवश्यकता भासल्यास ती राईट प्रोटेक्ट करून देण्यात यावी. परत घेताना पुन्हा ती न चुकता विषाणू विरहीत असल्याची खात्री करावी.

३.४ आपल्या कार्यालयास दिलेल्या संगणकावर नकली सॉफ्टवेअर लोड करू नये. विषाणूंचा प्रादुर्भाव मुख्यत्वे नकली सॉफ्टवेअरमुळे तर होतोच शिवाय **नकली सॉफ्टवेअर वापरल्याने फेरा कायद्याचे उल्लघंन होते.** नवीन विषाणू बऱ्याचदा विषाणू अज्ञावलीने उघडकीस येत नाहीत व त्यांचे निर्मूलन करण्यासाठी नवीन विषाणू निर्मूलन सॉफ्टवेअर विकत घ्यावे लागते व असे चक्र सतत चालू राहते. **नकली (Pirated) सॉफ्टवेअर वापरल्यास त्यामुळे उद्भवणाऱ्या कोणत्याही परिणामास आपण स्वत: सर्वस्वी जबाबदार असाल.**

३.५ आपल्या कार्यालयास देण्यात आलेले नॉर्टन (Norton) हे विषाणू निर्मूलन सॉफ्टवेअर Autoexexc.bat फाईलमध्ये समाविष्ट केल्याबाबत खात्री करून घेण्यात यावी. संगणक कार्यान्वित होत असताना प्रत्येकवेळी Autoexec.bat फाईल कार्यान्वीत केली जात असल्याने विषाणू निर्मूलन अज्ञावली आपोआप कार्यान्वीत होते व त्यामुळे संगणकाची विषाणूंबावत वारंवार तपासणी होते.

३.६ तसेच जे संगणक सर्व्हरला जोडण्यात आलेले आहेत अशा संगणकावर काम करताना सर्व कामे सर्व्हरवरच करण्यात यावी. कारण सर्व्हरवर विषाणू चिकीत्सा व निर्मूलनाचे काम नियमितपणे केले जाते.

३.७ सर्व संगणकांवर नॉर्टन ॲन्टी व्हायरस-२००१ हे सॉफ्टवेअर लोड करण्यात यावे.

३.८ नवीन विषाणूंचा प्रादुर्भाव टाळण्यासाठी ठराविक कालावधीनंतर व्हायरस डेफिनेशन फाईलचे अपडेशन करणे आवश्यक आहे.

GR-20020412155551080-0107

३.९ डेस्कटॉपवरील सर्व सिस्टिम्स विषाणूंकरिता आपोआप स्कॅन होतील अशाप्रकारे व्यवस्थ करण्यात यावी.

३.१० ई-मेल सोबत आलेली सहपत्रे उघडतांना योग्य काळजी घेणे गरजेचे आहे. आपणास अज्ञात व्यक्ती अथवा संस्थांकडून आलेले ई-मेल व सहपत्रे उघडू नयेत.

३.११ विषाणूंचा प्रादुर्भाव टाळण्यासाठी संगणकाची हार्डडिस्क पूर्णपणे शेअर करु नये

३.१२ माहिती तंत्रज्ञान संचालनालयाने प्रमाणित केलेल्या सॉफ्टवेअर शिवाय इतर सॉफ्टवेअ संगणकावर लोड करु नयेत. जर असे सॉफ्टवेअर लोड करण्याची आवश्यकता भासल्यास माहित तंत्रज्ञान संचालनालयाची पुर्वमान्यता घेण्यात यावी.

३.१३ संगणक विषाणूंमुळे बाधित झालेली माहिती मूळ स्वरुपात भरण्यासाठी आपणास आवश्य असलेल्या सर्व फाईल्सचे बॅकअप वारंवार ठराविक कालावधीत घेणे आवश्यक आहे. बॅकअप साधारणपणे दोन संच (सेट) असावेत.

४. संगणकावर नॉर्टन ॲन्टी व्हायरस २००१ रन करण्यासाठी पढील प्रमाणे कार्यवाही करावी

४.१ विंडोजमध्ये Start क्लिक करावे.
४.२ नंतर Program क्लिक करावे.
४.३ नंतर नॉर्टन ॲन्टी व्हायरस क्लिक करावे.
४.४ नंतर नॉर्टन ॲन्टी व्हायरस २००१ क्लिक करावे.
४.५ नंतर Scan For Virus क्लिक करावे व आवश्यकतेनुसार ड्राईव्ह निवडावा (A, C इ. सर्वसाधारणपणे)
४.६ शेवटी Scan My Computer क्लिक करावे.

५. संगणकातील बूट सेक्टरमध्ये विषाणूंचा प्रादुर्भाव होऊ नये म्हणून बूट सेक्टरला Inoculatio करावे. यामुळे बूट सेक्टरमधील महत्त्वाच्या असलेल्या Command.com व इतर फाईल्सच बाईट्सची संगणक सतत पाहणी करतो . या फाईल्सच्या बाईट्समध्ये बदल झाला असेल तर लगे संगणक तशी सूचना देतो. त्यामुळे विषाणूंपासून संगणकाचे संरक्षण होते. Inoculation करण्यासा पढील पद्धत वापरावी.

५.१ विंडोजमध्ये Start क्लिक करावे.
५.२ नंतर Program क्लिक करावे.
५.३ नंतर नॉर्टन ॲन्टी व्हायरस क्लिक करावे.
५.४ नंतर नॉर्टन ॲन्टी व्हायरस २००१ क्लिक करावे.
५.५ नंतर Options क्लिक करावे.
५.६ नंतर Other या शीर्षाखालील Inoculation क्लिक करावे.

५.७ Inoculation करावयाची फाईल निवडावी व क्लिक करावे.

६. मंत्रालय व परिसरातील कार्यालयासांठी मे. लॉरेन कंपनीशी फॅसिलिटी मॅनेजमेंट संदर्भात करार करण्यात आलेला असून सदर कंपनीने नवीन प्रशासकीय भवन येथे ११ व्या मजल्यावर हेल्पडेस्क उपलब्ध केलेला आहे. त्याचा विस्तार क्रमांक ३९७५ व ३९७५ असा आहे. राज्यातील इतर कार्यालयांनी या संचालनालयाच्या क्र. सीओएम-१००१/प्र.क्र.१५२/०१/३९, दिनांक २५/१०/२००१ या शासन निर्णयानुसार फॅसिलिटी मॅनेजमेंट संबंधीचा करार करावा.

६.१ फॅसिलिटी मॅनेजमेंट करारानुसार नियुक्त केलेला अभियंता संगणकाच्या समस्येसाठी आला असता त्यास सदर संगणकावर विषाणूंचा प्रादुर्भाव आढळून आला आणि सदर संगणक वापरणारी व्यक्ती विषाणू निर्मूलनाबाबतचे सॉफ्टवेअर वापरत नसल्याचे आढळून आले आणि त्या अभियंत्याने सदर सॉफ्टवेअर लोड करण्यास सुचविले तर त्या व्यक्तीने ते सॉफ्टवेअर लोड करण्यासाठी सदर अभियंत्यास सहकार्य करावे.

६.२ संगणकमध्ये ॲंटी प्रोटेक्ट व्हा-रस स्कॅनर हा पर्याय इनेबल्ड केलेला असावा. जर असे नसेल किंवा सदर स्कॅन व्यवस्थित कार्य करत नसेल तर फॅसिलिटी मॅनेजमेंटच्या अभियंत्याशी संपर्क साधावा.

६.३ नवीन विषाणू आढळून आल्यास संगणक वापरणाऱ्या व्यक्तीने फॅसिलिटी मॅनेजमेंटच्या अभियंत्यास तसे कळवावे तसेच या संचालनालयाद्वारेही असा नवीन विषाणू आढळून आल्यास सर्व संबंधितांना कळविण्यात येईल.

महाराष्ट्राचे राज्यपाल यांच्या आदेशानुसार व नावाने,

(प्र. दि. सोहळे)
उपसचिव

प्रति,
राज्यपालांचे सचिव,
मुख्यमंत्री यांचे सचिव.
उपमुख्यमंत्री यांचे सचिव
सर्व मंत्री यांचे खाजगी सचिव
सर्व राज्य मंत्री यांचे स्वीय सहायक
शासनाचे मुख्य सचिव
शासनाचे सर्व अपर मुख्य सचिव / प्रधान सचिव / सचिव

*प्रबंधक, उच्च न्यायालय, मुळ शाखा, मुंबई
*प्रबंधक, उच्च न्यायालय, अपील शाखा, मुंबई
*प्रबंधक, लोकायुक्त व उप लोकायुक्त यांचे कार्यालय, मुंबई
*सचिव, महाराष्ट्र लोकसेवा आयोग, मुंबई
*सचिव, महाराष्ट्र विधानमंडळ सचिवालय (विधानसभा), मुंबई

*सचिव, महाराष्ट्र विधानमंडळ सचिवालय (विधानपरिषद), मुंबई
महालेखापाल-१ (लेखा व अनुज्ञेयता), महाराष्ट्र, मुंबई
महालेखापाल-२ (लेखा व अनुज्ञेयता), महाराष्ट्र, नागपूर
महालेखापाल-१ (लेखा परीक्षा), महाराष्ट्र, मुंबई
महालेखापाल-२ (लेखा परीक्षा), महाराष्ट्र, नागपूर
अधिदान व लेखा अधिकारी , मुंबई/लेखाकोष भवन, वांद्रे (पूर्व), मुंबई
निवासी लेखा परिक्षा अधिकारी, मुंबई
सर्व जिल्हा कोषागार अधिकारी,
सर्व विभागीय आयुक्त,
सर्व जिल्हाधिकारी,
सर्व जिल्हा परिषदांचे मुख्य कार्यकारी अधिकारी,
सर्व मंत्रालयीन विभाग,
मंत्रालयीन विभागांच्या नियंत्रणाखालील सर्व विभाग प्रमुख व कार्यालय प्रमुख,
सामान्य प्रशासन विभागातील सर्व कार्यसने,
निवड नस्ती (दोन प्रती).

एच-1080(4500-3-02)-3अ. GR-200404121555900-017